

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA)	
)	
v.)	No. 1:19-cr-356
)	
KWASHIE SENAM ZILEVU,)	The Honorable Rossie D. Alston Jr.
)	
Defendant.)	Sentencing: December 1, 2021
)	

POSITION OF THE UNITED STATES WITH RESPECT TO SENTENCING

The United States of America, through undersigned counsel and in accord with 18 U.S.C. § 3553(a) and the U.S. Sentencing Commission Guidelines Manual (“Guidelines”), hereby provides its position with respect to the sentencing of Kwashie Senam Zilevu (“Defendant”). The United States requests that this Court adopt the findings of the Pre-Sentence Investigation Report (“PSR”) with respect to the Base Offense Level and Specific Offense Characteristics, which results in an advisory Guidelines range with respect to incarceration of 21–27 months.

Based on that advisory Guidelines range and the § 3553(a) factors, a sentence of incarceration of 27 months is sufficient, but not greater than necessary, in this case. A sentence of 27 months for this defendant appropriately captures the seriousness of his decision to repeatedly use a credit card obtained using the identity of Matthew Brown, which he used to purchase more than \$58,000¹ in goods and services to benefit himself and people close to him. *See* Pre-sentence Investigation Report (“PSR”) ¶ 58.

¹As detailed in PSR ¶ 58, Defendant should be held accountable for a loss of \$86,896.18, “which represents the actual charges made on the [Matthew] Brown and [Clifford] Shingleton credit cards, which were in excess of those cards’ credit limits, as well as an intended loss of \$19,000 for the [Larry] Fudger credit card.” However, the inclusion of the losses attributable to acquitted conduct—the use of credit cards in Shingleton and Fudger’s names to make \$28,686.69 in purchases—does not increase Defendant’s offense level beyond that of the convicted conduct in

Accordingly, the United States asks this Court to impose a sentence of 27 months of incarceration, three years of supervised release, and full restitution and forfeiture as described in greater detail below.

I. Relevant Procedural History

On November 26, 2019, a federal grand jury convening in the United States District Court for the Eastern District of Virginia, Alexandria Division, charged Defendant, a 37-year-old resident of Woodbridge, Virginia, and former information technology specialist with the Internal Revenue Service (IRS), with three counts of Access Device Fraud, in violation of 18 U.S.C. § 1029(a)(5) and three counts of Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A(a)(1). On July 17, 2021, after a 4-day jury trial, Defendant was convicted on Count One of the indictment, Access Device Fraud, in violation of 18 U.S.C. § 1029(a)(5).

II. Factual Background

Evidence submitted at trial and the facts as outlined in the PSR prove that Defendant used an American Express credit card issued in the name of Matthew Brown to make \$58,209.49 in purchases. *See* Government Trial Exhibit (Gov. Tr. Ex.) 401; PSR ¶ 58. Over the course of a four-day trial, the jury was presented with documentary evidence and witness testimony with respect to the defendant's unlawful use of an American Express card obtained in the name of Matthew Brown, including more than one-hundred exhibits, as well as the testimony of victims Matthew Brown and a representative from American Express, cooperating witness Kwaku Blay ("Blay"), and the lead case agent, Special Agent Flannan Soden ("SA Soden").

Count One, \$58,209.49. *See* USSG § 2B1.1(b)(1)(D),(E). As such, while the Court may properly consider the undisputed loss of \$86,896.18, the \$58,209.49 figure is a sufficient predicate for an increase in offense level of 6. *Id.*

The documentary evidence showed that the defendant purchased flights from multiple airlines for himself and others close to him to travel both internationally and domestically. It also included receipts from multiple retail stores where Defendant made numerous purchases, records showing transfers of funds from the defendant's personal bank account to further his fraudulent scheme, and transaction details showing payments to entities the defendant exclusively controlled. *See, e.g.*, Gov. Tr. Exs. 10, 11–11-D, 20–45, 50, 50–A, 51, 52, 120. In addition to the inculpatory financial documentation submitted into evidence, multiple exhibits containing images of the defendant, captured by surveillance cameras located at retail stores, which conclusively showed Defendant using the credit card obtained in Matthew Brown's name. *See* Gov. Tr. Exs. 21–A, 22, 24-A.

More specifically, in addition to the thousands of dollars Defendant spent at airlines, he used the card in the name of the victim at Floor & Décor to purchase nearly \$4,000 worth of flooring, at BJ's Wholesale to the tune of \$3,450, online at Amazon Defendant spent over \$1,200, and racked up nearly \$8,000 in PayPal charges—all on a card he was never authorized to use or to obtain.

At trial, the real Matthew Brown testified that he had never been associated with the fictitious entity "Belview Auto," nor had he ever lived at 14520 General Washington, Woodbridge, Virginia (Defendant's home address), both of which were used to obtain the credit card in this victim's name. Further testimony by Mr. Brown made it pellucidly clear to the factfinders that he had not made any of purchases with the American Express credit card opened in his name and that he never authorized the defendant or anyone else to do so. Based on this testimony and additional evidence submitted, the jury rightly determined that the defendant violated the law.

Testimony by cooperating witness Blay helped explain to the jury how the fraudulent scheme was devised, orchestrated and carried out by the defendant. He explained the sophisticated ways in which Defendant used his knowledge of computers and technology to further the scheme and prevent its detection by employing computer programs (TeamViewer), cryptocurrency (Bitcoin), and even fictitious charities (rebuildafricanow.org), which evidence showed the defendant created with the express purpose to commit fraud. *See* ECF no. 105 at 12–15, 17–19, 20–21.

SA Soden rounded out the government’s case by providing clear, concise testimony about the evidence presented, from how the defendant’s criminal activities first came to light, to the exact loss amount suffered by Defendant’s victims. Perhaps most persuasively, SA Soden explained to the jury how the defendant admitted to him and Postal Inspector Jackie Palmer that he in fact received and used what evidence has now proved is the fraudulently obtained credit card in Matthew Brown’s name: The defendant “did acknowledge that he received the credit card in Matthew Brown's name in the mail and took it out of an envelope[]” and “[h]e stated that he used the card to make purchases.” *See* ECF no. 106 at 14. This admission is even more glaringly inculpatory when considering the cover story that the defendant thereafter relayed to investigators—that he was “authorized” to use the credit card in Matthew Brown’s name to repay a supposed \$10,000 loan from Kwaku Blay. The main problem with the cover story being that he spent nearly \$60,000 using this credit card. *Id* at 15.

III. Guidelines Calculation

As the Court is well aware, although the Guidelines are advisory, sentencing courts “must consult those Guidelines and take them into account when sentencing.” *United States v. Booker*, 543 U.S. 220, 261 (2005). Thus, at sentencing a court “must first calculate the Guidelines range.”

Nelson v. United States, 555 U.S. 350, 351 (2009). Here, the PSR found a base offense level of 6; a 6-level increase for a loss more than \$40,000, and no greater than \$95,000; a 2-level increase for an offense involving the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification; and an additional 2-level increase for Defendant's use of a sophisticated means in the commission of the offense. This results in a total offense level of 16 and an advisory Guidelines range of 21–27 months.

A. The PSR accurately applies a 6-level increase for a loss more than \$40,000, and no greater than \$95,000, pursuant to U.S.S.G. § 2B1.1(b)(1)(D)

Defendant has not objected or otherwise disputed that the PSR accurately concludes that he caused a loss which exceeds \$40,000 but is less than \$95,000. *See* PSR ¶ 58, 66. This fact is also well supported by the trial testimony of SA Soden. SA Soden testified and provided the jury with summary charts detailing the expenditures on the Matthew Brown American Express card which totaled \$58,209.49. *See* Gov. Tr. Exs. 11–11-D (American Express Statements from May 2016 through June 2017) and 401 (Summary of Purchases from Matthew Brown American Express card). Accordingly, the Court should apply a 6-level increase, bringing Defendant's offense level to 12.

B. The PSR accurately applies a 2-level increase for Defendant's unauthorized transfer or use of a means of identification unlawfully to produce or obtain any other means of identification, pursuant to USSG §2B1.1(b)(11)(C)(i).

Here, again, Defendant has not objected to the PSR's accurate conclusion regarding his unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification. *See* PSR ¶ 28, 35, 56, 68. As detailed in the Application Notes to USSG §2B1.1, for the purposes of the Sentencing Guidelines, "'means of identification' has the meaning given that term in 18 U.S.C. § 1028(d)(7), other than that such means of identification shall be of an actual (*i.e.*, not fictitious) individual, other than the defendant or a person for whose

conduct the defendant is accountable under § 1B1.3 (Relevant Conduct).” USSG §2B1.1 at 88.

In turn, 18 U.S.C. § 1028(d)(7) sets forth:

(7) the term “means of identification” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—

(A) name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029(e));

18 U.S.C. § 1028(d)(7)(A)-(D). Particularly relevant in the instant case is that 18 U.S.C. § 1028(d)(7)(D) relies on § 1029(e)(1) to define “access device” as meaning “any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be **used to initiate a transfer of funds** (other than a transfer originated solely by paper instrument)[.]” (emphasis added). As described in further detail below, this includes the online money transfer services Venmo and PayPal.

The record before the Court shows that Defendant did in fact transfer or use the means of identification belonging to Matthew Brown to produce or obtain another other means of identification. A 2-level increase is appropriate because, under the guidelines, when a defendant uses a means of identification (*e.g.*, a victim’s name) to obtain another means of identification (*e.g.*, an online money transfer account), such an increase is necessitated. *United States v. Auguste*, 392 F.3d 1266, 1268 (11th Cir. 2004) (holding that “a court *must* apply a two-level enhancement

if an offense involved ‘the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any means of identification.’”) (emphasis in original). The evidence adduced at trial proves that means of identification belonging to Matthew Brown were used by Defendant to produce or obtain money transfer accounts with Venmo and PayPal.

With respect to Venmo, SA Soden testified at trial that Venmo is “an online payment service[,]” which “you can send money to and from peers and make purchases at businesses.” *See* ECF no. 106 at 38. He went on to describe two means of identification belonging to Matthew Brown that were used to obtain the Venmo account—“a Social Security number and a date of birth.” *See* ECF no. 106 at 40. In addition, it is self-evident that Matthew Brown’s *name* was clearly used to open the Venmo account. Section 1028(d)(7) plainly identifies an individual’s name as a means of identification. *See* ECF no. 106 at 39 (Question: What’s the name listed as the registered information? Answer: Matthew Brown.); *see also* Gov. Tr. Ex. 77 (Venmo Account in the name of Matthew Brown).

Defendant’s unauthorized transfer or use of Matthew Brown’s means of identification to unlawfully produce or obtain another means of identification went even further—it was also unlawfully used to obtain a PayPal account. As an initial matter, SA Soden testified that PayPal is “an online mobile payment service where you can send payments to businesses and peer-to-peer[,]” *i.e.*, exactly what § 1029(e)(1) intends to include when defining an “access device” as “any card, plate, code, account number, electronic serial number, [etc.]” ... “that can be used to initiate a transfer of funds[.]” *See* ECF no. 106 at 16. Upon further questioning, SA Soden told the jury that PayPal transfers were effected using the American Express card in Matthew Brown’s name (itself a means of identification). *Id.* at 16-18. Specifically, the PayPal account obtained using Matthew Brown’s means of identification was used to transfer \$7,950, which includes transfers of

funds to Macrotele, an entity the Defendant admitted to owning. *Id.* Like his use of means of identification belonging to Matthew Brown to unlawfully obtain a Venmo account, Defendant also used Matthew Brown’s identity to obtain a PayPal account. To obtain the PayPal account, he needed to provide a payment method to PayPal. As evidence presented at trial proved, the name and account number contained on the access device Defendant already unlawfully possessed—the Matthew Brown American Express card ending in 2003—was used, enabling him to transfer thousands of dollars to himself through the entity Macrotele and other PayPal transactions. *Id.*

On separate occasions, Defendant used the credit card in Matthew Brown’s name (itself a means of identification), as well as Matthew Brown’s social security number and date of birth, to obtain at least two additional means of identification—Venmo and PayPal accounts. For that, a 2-level increase for Defendant’s unauthorized transfer or use of a means of identification unlawfully to produce or obtain any other means of identification, pursuant to USSG §2B1.1(b)(11)(C)(i), should be applied, bringing Defendant’s offense level to 14.

C. A 2-level increase for Defendant’s use of a sophisticated means, pursuant to USSG §2B1.1(b)(10)(C), should also be applied.

Guidelines section 2B1.1(b)(10)(C) provides for a 2–level enhancement to a defendant’s offense level if “the offense ... involved sophisticated means.” Examples of sophisticated means include “hiding assets or transactions, or both, through the use of fictitious entities...” USSG § 2B1.1 cmt. n. 9(B). A district court’s finding that a defendant used sophisticated means is reviewed for clear error. *United States v. Kontry*, 238 F.3d 815, 821 (7th Cir.2001). A defendant’s offense of conviction may involve “sophisticated means” even if not every aspect of his scheme was complex or intricate. *United States v. Edelmann*, 458 F.3d 791, 816 (8th Cir.2006). The enhancement applies if the “defendant’s total scheme was undoubtedly sophisticated.” *Id.* (internal quotation marks omitted); see *United States v. Weiss*, 630 F.3d 1263, 1279 (10th Cir.2010) (“The

Guidelines do not require every step of the defendant's scheme to be particularly sophisticated; rather, as made clear by the Guidelines' commentary, the enhancement applies when the execution or concealment of a scheme, viewed as a whole, is especially complex or especially intricate." (internal quotation marks omitted)); see *also United States v. Ghertler*, 605 F.3d 1256, 1267 (11th Cir.2010) (no requirement that defendant's individual actions be sophisticated); *United States v. Jackson*, 346 F.3d 22, 25 (2d Cir.2003) (concluding a credit card fraud scheme linking unelaborate steps in a coordinated way to exploit the vulnerabilities of the banking system was "sophisticated"). And particularly relevant for the instant case, courts have concluded that "the use of fake charities as shell entities is sufficient to support application of the sophisticated means enhancement." *United States v. Edwards*, 744 F. App'x 825, 826 (4th Cir. 2018).

To begin, as described above, Defendant used Macrotele, an entity that he admitted to controlling, to carry out his fraud scheme. There is nothing in evidence to support that this entity was ever engaged in any legitimate business activities. Rather, it is clear that Defendant used Macrotele to effect several fraudulent transactions to benefit himself. He did so by creating multiple accounts in victim Matthew Brown's name to disguise his fraudulent activity and to transfer funds to himself (via Macrotele). Defendant's use of fictitious entities did not stop there. As cooperating witness Blay testified at trial, "[Defendant] had a website -- charity website, I believe was rebuildafricanow.org, rebuildafricanow.org, that we basically we had donation spots that we can go there and use approved cards to donate and the money comes into his own PayPal account." See ECF no. 105 at 20-21. Blay went on to explain that Defendant created this fictitious charity website and it "was just basically for us to be able to get the funds off the approved credit

cards that came in.” *Id.* at 21. Providing further detail of Defendant’s sophistication, Blay continued:

So for the website, it's -- it looks legitimate, like a charity-owned website that has donation 1,500, 2,000 or 800. So basically, you go in there and we used the cards that came in the mail that got approved and we donate money.

So let's say if you donate 1,500, he controls the website, so he knows, oh, like, he has an account attached to the website whereby if the funds go through in a day or two, it comes into his account.

Id.

While the government submits that Defendant’s use of these two fictitious entities is more than sufficient to apply §2B1.1(b)(10)(C)’s 2-level increase, Defendant also engaged in additional conduct that further demonstrates that the offense involved the use of sophisticated means. More specifically, from inception, use of a fictitious entity was integral to Defendant’s scheme. That entity, of course, is Belview Auto, the fictitious business used, alongside Defendant’s home address, to obtain the credit card in Matthew Brown’s name. *See* Gov. Tr. Ex. 10 (American Express Application); *see also* 11–11-D (American Express Statements from May 2016 through June 2017). Using this fictitious entity not only helped enable Defendant to obtain the credit card to begin with, each and every time he presented this credit card at a retail establishment—and there were many times (BestBuy, Floor & Décor, Lowe’s, BJ’s, etc.)—his passing this off as a business/corporate credit card was a sophisticated way to add an additional veneer of legitimacy to his illicit activities.

Defendant should receive a 2-level increase due to his use of a sophisticated means, pursuant to USSG §2B1.1(b)(10)(C), for using Macrotele, a fictitious African charity, and Belview Auto to carry out his fraudulent scheme, bringing his total offense level to 16. With a total offense level of 16 and a criminal history category of I, the advisory Guidelines range with respect to incarceration is 21–27 months.

III. Section 3553(a) Factors

As the Court is well aware, after calculating the Guidelines, a sentencing court must then consider that Guidelines range, as well as the sentencing factors set forth in § 3553(a), and determine a sentence that is appropriate and reasonable for the individual defendant. *Nelson*, 555 U.S. at 351; *see also United States v. Hughes*, 401 F.3d 540, 546 (4th Cir. 2005). With respect to 18 U.S.C. § 3553(a)'s enumerated factors, of particular pertinence here are the “nature and circumstances of the offense,” the need for the sentence “to reflect the seriousness of the offense,” “the history and characteristics of defendant,” the need “to promote respect for the law,” and the need for the sentence “to afford adequate deterrence to criminal conduct.” § 3553(a)(1), (a)(2)(A), (a)(2)(B), (a)(7). As explained below, based on those factors, a sentence of 27 months is warranted, appropriate, and reasonable.

A. A sentence of 27 months is necessary based on the nature, circumstances, and seriousness of the offense.

The defendant's crime was certainly serious; indeed, this was a crime of greed that simply never had to happen. There were countless opportunities for Defendant to mitigate this fraud, but he chose not to do so. Time and time again, Defendant used a credit card in the name of Matthew Brown to make what can only be described as lavish purchases. From taking elaborate international vacations and staying at luxury hotels, to hiring an interior designer to decorate his home, he just kept spending. Given Defendant's greed and the sophistication with which he carried out his fraud scheme, it is difficult to surmise when Defendant's fraud would have ended, but for the intervention of law enforcement.

Now, the defendant may come before the Court and claim that someone else (namely Kwaku Blay) is more culpable than he is. That argument does not serve to justify his actions and it is not borne out by the facts, especially in light of Mr. Blay's compelling testimony at trial—

testimony that was corroborated by independent evidence. And the fact remains that Blay lacks the advanced, highly technical education and expertise that Defendant possess, which was undoubtedly used to further the offense. Any argument to the contrary demonstrates nothing more than a defendant who is incapable of being honest with this Court, and himself.

B. A sentence of 27 months is necessary in light of the defendant's personal history and characteristics.

A sentence of 27 months is also necessary in light of the defendant's personal history and characteristics. At trial, defense counsel made much of his client's background and previous successes obtaining an advanced education and employment as an information technology specialist at the Internal Revenue Service (IRS). Indeed, such achievements are commendable. But what those previous accomplishments show more than anything is that the defendant's crime was due to nothing more than pure and utter greed. As defense counsel's closing argument emphasized, Defendant made quite a good living—well more than \$100,000 a year. But instead of living a life as a law-abiding citizen and enjoying the fruits of legitimate gainful employment, he chose to use his knowledge of computers and technology to engage in an elaborate fraud scheme. And the reason for that choice is clear—his greed, coupled with a lack of respect for the law, and a perception that he was too smart to get caught.

It is apparent from his attempts to deflect blame onto others that the defendant does not fully grasp the extent of his criminal conduct. Obviously, the defendant had the constitutional right to proceed to trial and to hold the government to its burden. However, to date, he has consistently refused to take responsibility for his actions. Nevertheless, it is apparent that a person with the defendant's educational background and training who held himself up as a shining example of success for his family never needed to resort to criminal activity. This defendant did anyway.

C. *A sentence of 27 months is necessary to promote respect for the law and afford adequate specific deterrence.*

The need for specific deterrence also warrants a sentence of 27 months. Specific deterrence is important in any fraud case, but it is an especially important factor for crimes like the defendant's, which are difficult to detect because the very factors that enable the criminal conduct to occur also aid in its concealment. That is, after all, why people like the defendant—sophisticated, educated individuals—commit such crimes. They do so because they believe the personal financial benefit to them outweighs the likelihood of getting caught and the duration of any potential imprisonment when caught.

Crimes like this one require conscious, repeated decision making, and defendants like this one make conscious, repeated decisions to act illegally. This is plainly shown from the defendant's frenetic ability, once he obtained a fraudulent credit card, to create numerous additional accounts, including those to transfer funds and others to help perpetuate his scheme, such as email addresses in a victim's name. At each turn, he schemed and devised additional opportunities to maximize and continue his fraud. Going to great lengths, such as making minimum payments on the credit card opened in Matthew Brown's name to keep the account open, extend the credit limit, and continue his scheme as long as possible.

Lastly, with respect to the recommend sentence of incarceration, to the extent that the defense argues that Defendant has already suffered the collateral consequence of losing his employment at the IRS, the government submits that that fact does not obviate the need for, and the deterrent effect of, a significant term of incarceration. Moreover, the importance of a stiff punishment is further underscored by the need to specifically deter Defendant from committing future crimes. He has shown the ability and impulse to turn to fraudulent activity even when facing no economic difficulty, and in light of his conviction, a significant period of incarceration will

send a message to Defendant and other would-be Kwashie Zilevus that crimes in which a victim's personally identifiable information is used, without any regard for the impact on that person, will not be tolerated. A term of imprisonment of 27 months is thus necessary to send a message that if the defendant again commits crimes like this one, he will again be met with a significant term of incarceration.

IV. Restitution and Forfeiture

Restitution

The defendant does not contest the loss amount contained in the attached proposed restitution order of \$49,771.02 and agrees to the payment terms contained therein. Accordingly, the United States submits that the Court's adoption of the findings of the PSR is sufficient to establish the loss to the victim by a preponderance of the evidence. In addition, American Express employee Peter Boresky testified to the loss at trial, and SA Soden provided the jury testimony detailing the losses to the victims through the introduction of Government Exhibit 401.

Forfeiture

Based upon an agreement between the government and the defendant, the United States also has attached a consent order of forfeiture to its sentencing position which requests that the Court enter a money judgment against the defendant in the amount of \$49,771.02. This forfeiture amount reflects proceeds of the fraud.

The basis for the forfeiture amounts was established at trial through the testimony of Peter Boresky and SA Soden's introduction of Government's Exhibit 401.

Consent Restraining Order

Lastly, as part of the above-mentioned agreement to resolve the monetary penalty aspects of the instant case, the parties consent to entry of the attached proposed restraining order and, accordingly, the government hereby moves for its entry by the Court.

V. Conclusion

For the reasons stated, the United States requests that this Court impose a term of incarceration of 27 months, three years of supervised release, restitution as outlined above, and forfeiture as requested in the government's separate motion.

Respectfully submitted,

Jessica D. Aber
United States Attorney

By: _____/s/
Ronald P. Fiorillo II
Jamar K. Walker
Counsel for the United States
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: (703) 299-3700
Fax: (703) 299-3980
Email: ron.fiorillo@usdoj.gov
Email: jamar.k.walker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on November 24, 2021, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will then send a notification of such filing (“NEF”) to all counsel of record.

By: _____/s/_____
 Ronald P. Fiorillo II
 Assistant United States Attorney